IFW AF

TRANSMITTAL LETTER
(General - Patent Pending)

Docket No.
VF-03272 (ES-00014)

In Re Application Of: **Peterson et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/886,302	6/21/2001	Shin Hon Chen	28581	2131	5599

Title: **CONDITIONING THE EXECUTION OF AN EXECUTABLE PROGRAM UPON SATISFACTION OF CRITERIA**

COMMISSIONER FOR PATENTS:

Transmitted herewith is:

Substitute Brief on Appeal (in triplicate);
transmittal letter;
certificate of mailing;
postcard

in the above identified application.

☒ No additional fee is required.

☐ A check in the amount of is attached.

☒ The Director is hereby authorized to charge and credit Deposit Account No. **50-2061** as described below.

- ☐ Charge the amount of
- ☒ Credit any overpayment.
- ☒ Charge any additional fee required.

☐ Payment by credit card. Form PTO-2038 is attached.
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

William H Meise
Signature

Dated: **10/4/2005**

William H. Meise
Reg. No. 27,574
Duane Morris LLP
P.O. Box 5203
Princeton, NJ 08543-5203
609-631-2453

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

10/4/2005.
(Date)

Susan Barlett
Signature of Person Mailing Correspondence

Susan Barlett
Typed or Printed Name of Person Mailing Correspondence

cc:

CERTIFICATE OF MAILING BY FIRST CLASS MAIL (37 CFR 1.8) Applicant(s): **Peterson et al.**	Docket No. **VF-03272 (ES-00014)**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit
09/886,302	**6/21/2001**	**Shin Hon Chen**	**28581**	**2131**

Invention: **CONDITIONING THE EXECUTION OF AN EXECUTABLE PROGRAM UPON SATISFACTION OF CRITERIA**

I hereby certify that this **Substitute brief on appeal (in triplicate); certificate of mailing; postcard**
(Identify type of correspondence)

is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on **10/4/2005**.
(Date)

Susan Barlett
(Typed or Printed Name of Person Mailing Correspondence)

Susan Barlett
(Signature of Person Mailing Correspondence)

Note: Each paper must have its own certificate of mailing.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPLICATION OF	:	Peterson et al.
SERIAL NUMBER	:	09/886,302
FILED	:	June 21, 2001
FOR	:	CONDITIONING THE EXECUTION OF AN EXECUTABLE PROGRAM UPON SATISFACTION OF CRITERIA
EXAMINER	:	Shin Hon Chen
Art Group	:	2131

SUBSTITUTE BRIEF ON APPEAL

1. REAL PARTY IN INTEREST

The application is assigned to Lockheed Martin Corporation, and was recorded on June 21, 2001 at Reel 011956, frame 0520.

2. RELATED JUDICIAL OR ADMINISTRATIVE PROCEEDINGS

None

3. STATUS OF CLAIMS

The application was originally filed with 10 claims, of which claims 1 and 9 were independent. In a first Office Action, all claims were rejected. In response, independent claims 1 was cancelled, claims 2 and 10 were amended to independent form, and changes to the dependency of other claims were made. A final Office Action continued the rejection of claims 2-8 and 10.

Appeal is taken from the rejection of claims 2-8 and 10.

4. STATUS OF AMENDMENTS

No amendments after final rejection are made.

5. SUMMARY OF THE INVENTION

The invention relates to a method for tending to reduce the possibility of virus infection of an intranet which communicates by way of a virtual private network (VPN) with a remote computer which is used for other purposes. The remote computer is subject to the possibility of infection, which infection might be communicated to the intranet through the VPN (page 5, line 7 to page 7, line 6).

According to an aspect of the invention, the underlying VPN-generating program (or other executable program) is appended to, or "encapsulated" in an executable policy enforcement agent including a header, an execution portion, and a data portion, to thereby form a combined program (page 7, line 8 to page 8, line 7). Another view of the encapsulation is that of substitution of the header of the policy enforcement agent for the header of the underlying application. The purpose of the encapsulation is to reduce the possibility of direct invocation of the underlying program and thereby avoiding the policy. In the context of the VPN-generating program, this corresponds to preventing execution until an antivirus program has executed. When the underlying program is to be invoked, the combined program is invoked (page 9, lines 25-30), which in turn invokes the policy enforcement agent. The policy enforcement agent requires that the policy be fulfilled, as for example by running an antivirus program, before allowing execution of the underlying program, such as the VPN-generating software (page 9, line 30 to page 10, line 8).

An advantage of the encapsulated executable program according to an aspect of the invention is that it can be moved from one computer to another, without requiring any changes to the new or receiving computer, and the encapsulated program will, in the new computer, have the same effect as in the old computer.

6. SUMMARY OF THE CLAIMED SUBJECT MATTER

The independent claims on which appeal is sought are claims 2 and 10.

Claim 2 recites

A security method for controlling use of an executable application (page 19, lines 12; FIGURE 3, item 300), said method comprising the steps of:

procuring a software executable policy enforcement agent (also referred to as PEA and "control module" - page 7, lines 10, 13, 15, 20, 24, 28, 31, 32; page 8 lines 4, 10; page 9, lines 1, 6, page 10 lines 24, 28; page 13, lines`13, 14; page 19, lines 18, 25; page 20, line 13, 23, 28; page 21, lines 1, 6, 11; page 22, line 18; and FIGURE 4, item 410) which, when invoked, imposes one or more conditions (page 1, line8; page 8, lines 4, 13, 18, 31; page 9, lines 17, 29; page 20, line 16; FIGURE 5, items 514, 520) on successful execution, and which, when successfully executed, invokes execution of said executable application (page 8, line 15; page 20, line 16; FIGURE 5a, item 522; FIGURE 5b, item 522)

encapsulating (page 7, line 19; page 8, line 19; page 10, line 24; page 14, line5; page 19, line 17; page 20, line 23; page 22, line 19; FIGURE 4 executable application 300 is encapsulated or lies within combined program 400) said executable application (300 of FIGURES 3 and 4) with said policy enforcement agent (410 of FIGURE 5) without changing said executable application (300 of FIGURE 3), to thereby produce a combined program (400 of FIGURE 5);

substituting (page 7, line 25; page 8 line 23; page 9, lines 5, 24; page 20, line 27; page 21, lines 9, 31) said combined program (400 of FIGURE 5) for said executable application (300 of FIGURE 3), so that said policy enforcement agent (410 of FIGURE 5) executes instead of said executable application program (300 of FIGURE 3) when said executable application (300 of FIGURE 3) is invoked; and

one of (a) satisfying said conditions of said control module (page 8, line 31; page 13, lines 26, 27, 30; page 14, line 2, 5; page 15, lines 10, 12, 18, 24; page 16, line 2; page 18, lines 5, 7, 22; page 20, line 4, 8; page 21, line 3; page 22, line 28), whereby said executable application (300 of FIGURE 3) executes, and (b) not satisfying said conditions, whereby said executable application does not execute (page 8, line 33 to page 9, line 3; page 21, lines 5-8);

wherein said software executable policy enforcement agent (410 of FIGURE 4) includes a header component (412 of FIGURE 4), and said substituting step includes the step of amending said header component (310 of FIGURE 3) of said policy enforcement agent portion (410) of said *combined program (400) to match the characteristics of said combined program (400).*

Claim 10 recites

A method for policy enforcement in relation to an executable application (300 of FIGURE 3), said method comprising the steps of:

procuring a software control element (400) which is identifiable to a host operating system as an executable program (page 7, lines 12-15;) and which includes an execution component (300;414) for executing said executable application (400), and which also contains a set of conditions (514 of FIGURE 5a, 520 of FIGURE 5b) which must be met in order to invoke said executable application (400);

combining said software control element with said executable application (300; page 8, lines 18-26; page 20, lines 18-26), to form a combined program (400);

substituting (page 7, line 25; page 8 line 23; page 9, lines 5, 24; page 20, lines 26-31; page 21, lines 9, 31) said combined program (400) for said executable application (300 of FIGURE 3; page 8, lines 21-27);

commanding execution of said combined program (page 8, lines 26-33; page 20, line31-page 21, line2), to thereby execute said software control element, whereupon said execution component is invoked if said conditions are met, *and said executable application executes (page 21, lines 2-5);*

wherein software control element (410) includes a header (412) identifying the locations of executable and data portions (page 14, lines 17-23, page 15, lines 15-21) of said control element (410), and said step of combining said software control element with said executable application includes the steps of:

appending said executable application to said software control element (page 14, lines 17-23, page 15, lines 15-21) in a location identified by said software control element as a data location (page 15, lines 23-28); and

updating said header of said software control module (page 15, lines 23-28) to correspond with the characteristics of said combined program.

No means-plus-function or step-plus-function terms appear in the claims.

7. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 2 and 10 are patentable in a 35 U.S.C. §102(e) sense over the cited O'Brien et al. reference.

2. Claims 3-8 and 10 are patentable in a 35 U.S.C. §103(a) sense over O'Brien in view of Kayashima et al. and further in view of Eggbraaten et al. and other references.

8. GROUPING OF CLAIMS

Claims 2 and 10 stand or fall separately. Claims 3-8 stand or fall together, but separately from claims 2 and 10.

9. ARGUMENT

9A. The References

The O'Brien reference (U.S. 6,658,571) is a computer security system, in which access to computer resources such as processing units, ROM, RAM, or busses are selectively withheld from operating programs (column 3, lines 2-25, 39-49) by security modules if they execute malicious software. Note that the security modules (105) can be loaded within kernel 102 while computer system 100 is running (column 3, lines 56-64) to provide the security function as to an executing underlying programs 107. In short, O'Brien et al. selectively withhold computer resources from currently running underlying programs in accordance with their security programming.

9B. Anticipation

There is a salient difference between the claimed arrangement and the O'Brien arrangement. Note that security in O'Brien et al. depends upon the security modules 105 of FIGURE 1 of O'Brien, which are preloaded into kernel 102 (column 3, lines 55-56), apart from applications 107, which execute in user space (column 3, lines 29-37). Thus, the simple transfer of an application, such as 107 of O'Brien et al., to a new computer, will not transfer the security aspects as in the arrangement of the claimed invention. Instead, other measures must be taken, such as additionally transferring the security module. As to any particular application, the security is provided by software preloaded into the computer, rather than by the encapsulated program or application itself. These differences arise from the recitations of the claims, as set forth below.

Claims 2 and 10 are rejected as anticipated by O'Brien et al. Claim 2 as amended recites inter alia

> "substituting said combined program for said executable application, so that said policy enforcement agent executes instead of said executable application program when said executable application is invoked; and
>
> one of (a) satisfying said conditions of said control module, whereby said executable application executes, and (b) not satisfying said conditions, whereby said executable application does not execute;
>
> wherein said software executable policy enforcement agent includes a header component, and said substituting step includes the step of amending said header component of said policy enforcement agent portion of said combined program to match the characteristics of said combined program."

It does not appear that the O'Brien arrangement meets any of these limitations of claim 2. More particularly, it appears that the O'Brien software program(s) execute(s) independently of the security modules, as the security modules have nothing on which to act unless the underlying programs make calls for system resources, which can only occur if the underlying programs are already running. Thus, the security modules do not alternatively

> "(a) satisfy[ing] said conditions of said control module, whereby said executable application executes, and (b) not satisfying said conditions, whereby said executable application does not execute"

as recited in claim 2

Further, Examiner states (Final Rejection, page 3)

> "O'Brien further discloses wherein said software executable policy enforcement agent includes a header component, and said substituting step includes the step of amending said header component of said policy enforcement agent portion of said combined program to match the characteristics of said combined program (O'Brien: column 2 lines 12-38 . . ."

Examiner is clearly wrong in this regard, as O'Brien makes no mention whatever of "header" or "substitution." Thus, each and every element of claim 2 is not found in O'Brien, and the requirements of anticipation are not met. In the absence of a showing in O'Brien of each and every element of claim 1, there can be no anticipation.

Claim 2 is clearly patentable in a 35 U.S.C. §102(e) sense over O'Brien. Since Examiner indicates that claim 10 has the same scope as claim 2, claim 10 is also patentable.

9C. Obviousness

Examiner premises the 35 U.S.C. §103(a) rejection of dependent claims 3-8 on the same principal reference (O'Brien et al.) as that used for the anticipation rejection. As argued above, independent claims 2 and 10 are patentable in an anticipation sense. Thus, dependent claims 2-8 depend from patentable parent claim 2, and they are patentable therewith.

Aside from the dependency of claims 3-8 from patentable claim 1, Examiner has made no showing of a proper nexus for his suggested combination of O'Brien et al. with Kayashima and Eggebraaten. Examiner's statement in §8 on page 4 of the Final Rejection is

> "O'Brien does not explicitly disclose wherein said executable application includes a VPN-tunneling-generating application, ... However, Kayashima discloses running antivirus and firewall security policy procedures to perform security management . . . . It would have been obvious to one skilled in the art . . . to run antivirus program as security measure to determine whether the application is allowed to execute on the computer system."

But, as mentioned above, O'Brien does not prevent the starting of the executable program, it merely evaluates the result of the executing program for security purposes. Thus, O'Brien is incompatible with Examiner's suggested interpretation of Kayashima, and it would not be obvious to combine them. Claims 3-8 are patentable in a 35 U.S.C. §103 sense over O'Brien in view of Kayashima, and therefore over suggested combinations of O'Brien with Kayashima and other references.

10. AUTHORITIES RELIED UPON

For the proposition that there must be identity of each and every element of the claimed invention and the reference in order to find anticipation, appellant relies upon one or more of RCA Corp. v Applied Digital Data Systems, Inc. 221 USPQ 385, 388 (Fed. Cir. 1984); Kalman v Kimberly-Clark Corp., 218 USPQ 781, 789 (Fed. Cir. 1983); Orthokinetics, Inc. v Safety Travel Chairs, Inc., 1 U.S.P.Q 2^{d} 1081, 1087 (Fed. Cir. 1986); Hybritech, Inc. v Monoclonal Antibodies, Inc., 231 USPQ 81, 90 (Fed. Cir. 1986); Carella v Starlight Archery & Pro Line Co., 231 USPQ 644, 646 (Fed. Cir. 1986).

For the proposition that a dependent claim is non-obvious if it depends from a patentable claim, appellants rely on In re Fine, 5 USPQ2d 1596, 1600 (Fed. Cir. 1988), citing Hartness Int'l v Simplimatic Eng'g Co., 2 USPQ2d 1826, 1831; In re Abele, 214 USPQ 682, 689 (CCPA 19820

11. CONCLUSION

Claims 2 and 10 are patentable in an anticipation sense over Examiner's suggested anticipatory reference. Examiner's rejection of claims 2 and 10 should be reversed, together with the rejection of dependent claims 2 to 8. Reversal of Examiner's rejection is requested.

12. Please charge the fee for the appeal brief to 50-2061.

Respectfully Submitted

William H. Meise
Reg. No. 27,574

IN TRIPLICATE

CLAIMS APPENDIX

1. (Cancelled) A security method for controlling use of an executable application, said method comprising the steps of:

procuring a software executable policy enforcement agent which, when invoked, imposes one or more conditions on successful execution, and which, when successfully executed, invokes execution of said executable application;

encapsulating said executable application with said policy enforcement agent without changing said executable application, to thereby produce a combined program;

substituting said combined program for said executable application, so that said policy enforcement agent executes instead of said executable application program when said executable application is invoked; and

one of (a) satisfying said conditions of said control module, whereby said executable application executes, and (b) not satisfying said conditions, whereby said executable application does not execute.

2. (Previously Amended) A security method for controlling use of an executable application, said method comprising the steps of:

procuring a software executable policy enforcement agent which, when invoked, imposes one or more conditions on successful execution, and which, when successfully executed, invokes execution of said executable application;

encapsulating said executable application with said policy enforcement agent without changing said executable application, to thereby produce a combined program;

substituting said combined program for said executable application, so that said policy enforcement agent executes instead of said executable application program when said executable application is invoked; and

one of (a) satisfying said conditions of said control module, whereby said executable application executes, and (b) not satisfying said conditions, whereby said executable application does not execute;

wherein said software executable policy enforcement agent includes a header component, and said substituting step includes the step of amending said header component of said policy enforcement agent portion of said combined program to match the characteristics of said combined program.

3. (Previously Amended) A method according to claim 2, wherein said executable application includes a VPN-tunnel-generating application, and said step of satisfying said conditions includes the step of running an antivirus program.

4. (Previously Amended) A method according to claim 2, wherein said executable application includes a VPN-tunnel-generating application, and said step of satisfying said conditions includes the step of running an antivirus program having an acceptable update status.

5. (Previously Amended) A method according to claim 2, wherein said step of satisfying said conditions includes the step of running a personal firewall program.

6. (Previously Amended) A method according to claim 2, wherein said executable application accepts verification information in a format other than a digital certificate, and said step of satisfying said conditions includes the step of accepting a digital certificate.

7. (Original) A method according to claim 6, wherein said step of accepting a digital certificate includes the step of accepting an X.509 based digital certificate.

8. (Original) A method according to claim 6, further comprising the step of translating at least some information from said digital certificate into a form recognizable by said executable application.

9. (Cancelled) A method for policy enforcement in relation to an executable application, said method comprising the steps of:

procuring a software control element which is identifiable to a host operating system as an executable program and which includes an execution component for executing said executable application, and which also contains a set of conditions which must be met in order to invoke said executable application;

combining said software control element with said executable application, to form a combined program;

substituting said combined program for said executable application;

commanding execution of said combined program, to thereby execute said software control element, whereupon said execution component is invoked if said conditions are met, and said executable application executes.

10. (Previously Amended) A method for policy enforcement in relation to an executable application, said method comprising the steps of:

procuring a software control element which is identifiable to a host operating system as an executable program and which includes an execution component for executing said executable application, and which also contains a set of conditions which must be met in order to invoke said executable application;

combining said software control element with said executable application, to form a combined program;

substituting said combined program for said executable application;

commanding execution of said combined program, to thereby execute said software control element, whereupon said execution component is invoked if said conditions are met, and said executable application executes;

wherein software control element includes a header identifying the locations of executable and data portions of said control element, and said step of combining said software control element with said executable application includes the steps of:

appending said executable application to said software control element in a location identified by said software control element as a data location; and

updating said header of said software control module to correspond with the characteristics of said combined program.

12. EVIDENCE APPENDIX

No evidence has been submitted pursuant to 37 C.F.R.§§ 1.130, 1.131, or 1.132.

13. RELATED PROCEEDINGS APPENDIX

No decisions have been rendered by a court or by the Board of Patent Appeals and Interferences in any related appeal or interference proceeding identified above.